

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
17 June 2004 (17.06.2004)

PCT

(10) International Publication Number
WO 2004/051593 A2

(51) International Patent Classification⁷: **G08C 17/00**

(21) International Application Number:
PCT/IB2003/005289

(22) International Filing Date:
19 November 2003 (19.11.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0228032.9 30 November 2002 (30.11.2002) GB

(71) Applicant (for all designated States except US): **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL];
Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **WILCOX, Martin, S.** [GB/GB]; c/o Philips Intellectual Property & Standards,
Cross Oak Lane, Redhill, Surrey RH1 5HA (GB).

(74) Agent: **SHARROCK, Daniel, J.**; Philips Intellectual
Property & Standards, Cross Oak Lane, Redhill, Surrey
RH1 5HA (GB).

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

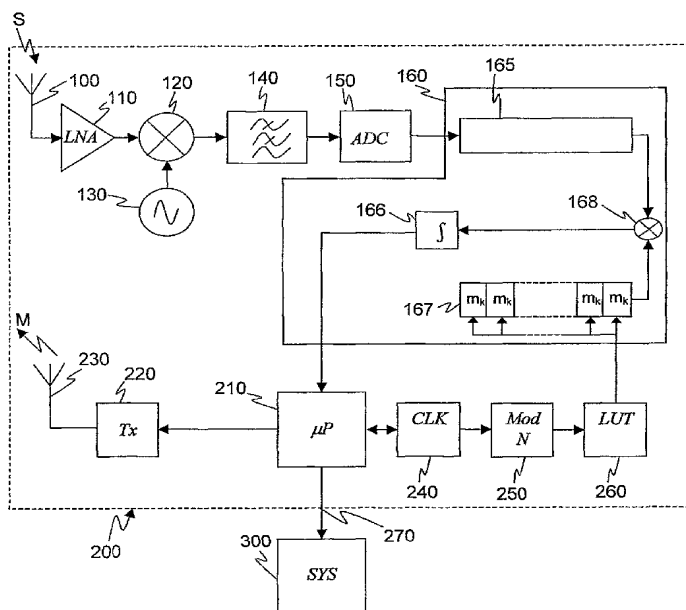
(84) Designated States (regional): ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:

— as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG,

[Continued on next page]

(54) Title: WIRELESS ACTIVATION SYSTEM, METHOD AND DEVICE



(57) Abstract: A wireless activation system, such as a keyless car entry system, uses repeated code sequences (mk) for communication between a transmitter device (400) and a receiver device (200). By varying the sequence duration in a synchronism at the transmitter device and receiver device, either by varying the number of symbols or chips in the sequence, or by varying the symbol or chip rate, it is made more difficult for an unauthorised party to detect the code sequences and relay the code sequences to achieve unauthorised activation at the receive device (200).

WO 2004/051593 A2



MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

Published:

— without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

DESCRIPTION

WIRELESS ACTIVATION SYSTEM, METHOD AND DEVICE

5 The invention relates to a wireless activation system, apparatus for use therein, and a method of wireless activation, which may be used, for example, for remote control applications such as wireless activation and deactivation of a lock on a vehicle door, or for tagging a person, animal or object.

10 Keyless car entry systems, in which the proximity of the car owner with a key fob in his pocket is sufficient to unlock the car door, are becoming increasingly common-place. Such a system is illustrated in Figure 1 and uses two-way communication between the key fob 10 held by the car owner A and an in-car device 20. Typically, the in-car device generates a magnetic field M
15 using a 125 kHz signal so that it is limited to a range of a few metres. The key fob detects the magnetic field M and then responds with a UHF code signal S, for example in the range 800-900 MHz. When the in-car device is satisfied that a valid code signal S has been received from the key fob, the in-car device unlocks the car door. Alternatively, UHF or microwave frequency
20 bands could be used for both the car to key fob communication and the key fob to car communication.

 Keyless car entry systems can be extended to "Keyless Go" systems in which it is not even necessary to insert a key into an ignition switch in order to start the car's engine. Instead the driver presses a button and the car engine
25 starts only if the key fob is nearby.

 Known keyless car entry systems are susceptible to what is known as the "relay attack". Relay attack is illustrated in Figure 2. A thief C close to the car uses first relay attack apparatus 30 to detect the magnetic field M around the car and to pass the parameters P of the magnetic field M to an accomplice
30 B who is close to the owner A of the car. The accomplice B uses a second relay attack apparatus 40 to receive the parameters P of the magnetic field M and to generate a spurious magnetic field M' which mimics the magnetic field

M generated by the in-car device 20. The owner's key fob 10 responds by transmitting the code signal S, even though the owner A may be many hundreds of metres away from the car. The second relay attack apparatus 40 relays the code signal S to the first relay attack apparatus 30, which in turn
5 relays the code signal S to the in-car device 20. The in-car device 20 reacts to the code signal S by unlocking the car door, and the thief C is able to steal the car.

One method of mitigating against the relay attack is to measure the time of flight of the code signal S and to unlock the car door only if the time of flight
10 measurement indicates that the key fob is very close to the car. However, practical schemes for measuring the time of flight result in an ambiguity such that, by inserting a delay in the code signal S relayed from the key fob to the in-car device, the key fob can be made to seem closer to the car than it actually is. Therefore even known protection systems are vulnerable to relay
15 attack.

Tagging systems can also be vulnerable to relay attack. In such a system a person, animal or object is equipped with a transmitter device for transmitting a signal to a receiver device. The receiver device estimates the distance of the transmitter device and if the distance becomes larger than a
20 predetermined value, or alternatively, depending on the application, smaller than a predetermined value, an alert is generated. By means of a relay attack, the receiver device can be deceived into making a false estimate of distance.

An object of the present invention is to make relay attack more difficult.
25 According to a first aspect of the invention there is provided a wireless activation system comprising a first device having means for generating and transmitting a code signal, wherein each successive transmission of the code signal comprises a successive code sequence from a succession of code sequences, and a second device having means for generating the succession
30 of code sequences in synchronism with the first device, means for receiving the code signal, means for detecting the successive code sequence transmitted by the first device, means for generating an indication of the time

of flight of the code signal, and means for generating an activation signal in response to the combination of the detected successive code sequence corresponding to the successive code sequence generated most recently by the second device and the indication of the time of flight being within a
5 predetermined range of values, wherein the succession of code sequences comprises code sequences of different time durations.

According to a second aspect of the invention there is provided a method of wireless activation comprising at a first device generating and transmitting a code signal, wherein each successive transmission of the code
10 signal comprises a successive code sequence from a succession of codes, and at a second device generating the succession of code sequences in synchronism with the first device, receiving the code signal, detecting the successive code sequence transmitted by the first device, generating an indication of the time of flight of the code signal, and generating an activation
15 signal in response to the combination of the detected successive code sequence corresponding to the successive code sequence generated most recently by the second device and the indication of the time of flight being within a predetermined range of values, wherein the succession of code sequences comprises code sequences of different time durations.

20 According to a third aspect of the invention there is provided a transmitter device for use in a wireless activation system, comprising means for generating and transmitting a code signal wherein each successive transmission of the code signal comprises a successive code sequence from a succession of code sequences and wherein the succession of code
25 sequences comprises code sequences of different time durations. The term "transmitter device" does not exclude the possibility of the device also including a receiver, but is merely used for convenience to denote a device that suitable for generating and transmitting the code signal.

According to a fourth aspect of the invention there is provided a receiver
30 device for use in a wireless activation system, comprising means for generating a succession of code sequences, means for receiving a code signal, means for detecting a code sequence conveyed by the code signal,

means for generating an indication of the time of flight of the code signal, and means for generating an activation signal in response to the combination of the detected code sequence corresponding to the code sequence generated most recently and the indication of the time of flight being within a
5 predetermined range of values, wherein the succession of code sequences comprises code sequences having different time durations. The term "receiver device" does not exclude the possibility of the device also including a transmitter, but is merely used for convenience to denote a device that is suitable for receiving the code signal and, in response, generating the
10 activation signal.

Each code signal comprises a number of identical code sequences. By using code sequences of different durations in different code signals, it becomes more difficult for relay attack apparatus to predict the duration of a transmitted code sequence, the code sequence is more difficult for the relay
15 attack apparatus to detect, and the delay required to deceive the receiver device into being activated by a distant transmitter device is more difficult for the relay attack apparatus to calculate and insert in the relayed signal.

Code sequences of different durations may be implemented by using different numbers of symbols or chips in the code sequences, or by using
20 different symbol or chip rates.

The invention will now be described, by way of example only of a keyless car entry system, with reference to the following drawings in which:

Figure 1 is a schematic diagram of a wireless activation system,

25 Figure 2 is a signal flow diagram of a wireless activation system under relay attack,

Figure 3 is a block schematic diagram of a receiver device in accordance with the present invention for use in a wireless activation system,

Figure 4 is a block schematic diagram of a transmitter device in
30 accordance with the present invention for use in a wireless activation system, and

Figure 5 illustrates a succession of code signals.

First, an explanation is presented of how the ambiguity in the calculated time of flight arises. To illustrate this, we consider an example in which a code signal s_j $j=1,N$ is a direct sequence spread spectrum signal having a chip rate of 1Mchip/s and in which the transmit power of the transmitter device is -20dBm in order to ensure a long battery life. In order to enable the receiver device to be simple, rather than transmit a single, long code sequence, each code signal s_j comprises a short code sequence m_k $k=1,P$ repeated identically within the code signal s_j . For example, code signal s_1 can have a length of 10 chips corresponding to 10 μ s duration. In order to ensure reliable detection of the code signal s_j , the receiver device enables its receiver for a time window when the code signal s_j is expected to be received. In order to measure a distance of 10m to an accuracy of 1m using the power level of -20dBm, the receiver device typically needs to receive a signal of 1ms duration in order to average the noise sufficiently, so the duration of the receiver time window is chosen to be approximately 1ms. The precise time of arrival of the code signal s_j at the receiver device is uncertain due to the variable propagation distance of the code signal s_j , and to ensure that 1ms of signal is received when the receiver is enabled throughout the time window, the transmitted code signal s_j is longer than the time window, and comprises the code sequence m_k repeated for an overall duration of 2ms. The code signal s_1 with a constituent code sequence m_1 is illustrated in Figure 5.

A receiver device 200 suitable for use in an in-car device and adapted in accordance with the invention is illustrated in Figure 3. It comprises a transmitter (T_x) 220 coupled to an antenna 230 for radiating the magnetic field M and coupled to a processing means (μP) 210 such as a microprocessor for controlling generation of the magnetic field M. In addition there is a low noise amplifier (LNA) 110 for receiving the code signal s_1 from an antenna 100. An output of the LNA 110 is coupled to a first input of a mixer 120 where it is down converted by being mixed with a local oscillator signal generated by a local oscillator source 130 and coupled to a second input of the mixer 120. An output of the mixer is coupled to an input of a low pass filter 140 and an output

of the low pass filter 140 is coupled to an input of an analogue-to-digital converter (*ADC*) 150. An output of the *ADC* 150 is coupled to an input of a detector 160 for detecting the code signal s_j . The detector 160 comprises a buffer 165 for storing the part of the received code signal s_j received in the receiver time window and delivered from the output of the *ADC* 150. The detector 160 also comprises a cyclic register 167 for storing a reference code signal comprising identical concatenated code sequences m_k . An output from the buffer 165 and an output from the cyclic register 167 are coupled to respective inputs of a multiplier 168, an output of the multiplier 168 is coupled to an input of an integrator 166, and an output of the integrator 166 is coupled to an input of the processing means 210. In operation, correlation between the signal stored in the buffer 165 and the reference code signal stored in the cyclic register 167 is performed by multiplying these signals in the multiplier 168 and integrating the resulting product in the integrator 166, and repeating these steps for consecutive cyclic shifts of the reference code signal in the cyclic register 167. Due to the use of short code sequences m_k , a correlation peak occurs at the output of the integrator 166 within at most the number of cyclic shifts corresponding to the length of the code sequence m_k . The processing means 210 processes the correlation signal supplied to it by integrator 166 to identify the time of occurrence of the correlation peak and to estimate the time of flight of the code signal s_j . To enable the time of flight to be calculated the processing means 210 is coupled to a clock (*CLK*) 240. Signals detected by the detector 160 are used by the processing means 210 to adjust the clock 240 so that it is maintained in synchronism with the device transmitting the code signal (i.e. transmitter device 400 having a clock 440, described below in relation to Figure 4). From the time of flight the processing means 210 calculates the distance of the receiver device 200 from the key fob and if the distance is within a predetermined limit, generates an activation signal on an output 270 which is coupled to a car locking system (*SYS*) 300. The activation signal results in the car doors being unlocked.

Because the code signal s_j comprises identical concatenated code sequences m_k , a similar correlation peak is observed at the output of the

detector 160 if the code signal s_j is delayed by a multiple of the code sequence m_k duration, so there is an ambiguity in the calculated time of flight of the code signal s_j . In the case of code sequence m_1 of duration $10\mu\text{s}$, there is an ambiguity of $n \times 10\mu\text{s}$, where n is an integer. This results in an ambiguity of n
5 $\times 3\text{km}$ in the calculated propagation distance.

The ambiguity can be resolved by ensuring that the ambiguity is larger than any distance required to be measured and by subtracting units of the ambiguity distance away from the measured distance until a figure less than the ambiguity distance is obtained. For example, for a keyless car entry
10 system, only distances up to about 20m need to be measured as the system does not need to operate over longer distances. If the key fob is further away than 3km, insufficient signal power will propagate to the vehicle to enable a distance measurement to be made. If the measurement using the code sequence m_1 yields a propagation distance of 3.01km, it can be readily
15 concluded by subtracting the ambiguity distance of $n \times 3\text{km}$ that the key fob is 10m from the vehicle. However, under relay attack, the key fob may in reality be 3.01 km from the vehicle with the power level of the code signal boosted by the relay attack apparatus 30.

As another example, the key fob may be 1km from the vehicle, at which
20 distance the receiver device 200 should determine that it should not react to the code signal s_1 because the driver is too distant. However, a relay attack apparatus 30 or 40 could insert an additional delay of $6.7\mu\text{s}$ causing the receive device 200 to measure a distance of 3.01km and conclude, after allowing for ambiguity of $n \times 3\text{km}$, that the key fob is only 10m from the vehicle,
25 and therefore falsely allow access to the vehicle.

According to the invention, protection against relay attack is provided by arranging for the duration of the code sequence to vary. There is a predetermined set of code signals s_j , $j=1, N$, where each code signal s_j comprises a predetermined code sequence from the set of code sequences
30 m_k , $k=1, P$. The code sequences m_k are chosen to have a low cross correlation. The number of different durations of the code sequences m_k , and the number of different values P of the code sequences m_k , may be less than

N , i.e. the code sequences m_k need not be unique within the predetermined set of code signals s_j . The code signals s_j may be unique to a particular pair of transmitter device and receiver device, or the order in which the code signals s_j are transmitted may be unique to a particular pair of transmitter device and receiver device.

In the example embodiment, having transmitted a code signal s_1 comprising a code sequence m_1 of length 10 chips, the next code signal transmitted will be s_2 and will comprise a code sequence m_2 of length 11 chips. By using code sequence m_2 the time ambiguity increases to $11\mu\text{s}$ and the distance ambiguity increases by 300m to $n \times 3.3\text{km}$. Now if the key fob is 1km from the vehicle and a relay attack apparatus 30 or 40 inserts an additional delay of $6.7\mu\text{s}$, the receive device 200 will measure a distance of 3.01km and conclude, after allowing for ambiguity, that the key fob is 3.01km from the vehicle, and therefore not allow access to the vehicle.

The next code signal to be transmitted will be s_3 and will comprise a code sequence m_3 of length 9 chips. By using code sequence m_3 the time ambiguity decreases to $9\mu\text{s}$ and the distance ambiguity decreases by 300m to $n \times 2.7\text{km}$. Now if the key fob is 1km from the vehicle and a relay attack apparatus 30 or 40 inserts an additional delay of $6.7\mu\text{s}$, the receive device 200 will measure a distance of 3.01km and conclude, after allowing for ambiguity, that the key fob is 310m from the vehicle, and therefore not allow access to the vehicle. In this case, if the relay attack apparatus 30 or 40 is to succeed in deceiving the receive device 200 into concluding that the key fob was only 10m away, the relay attack apparatus 30 or 40 would need to insert an additional delay of $5.7\mu\text{s}$. By varying the duration of the code sequences m_k , it becomes more difficult for the relay attack apparatus 30 or 40 to detect the code signal s_j and more difficult to estimate and implement the delay required to deceive the receiver device 200. In Figure 5, the code signals s_1 , s_2 and s_3 are illustrated, together with a generalised code signal s_j comprising code sequences m_k .

Referring to Figure 4, there is shown a block schematic diagram of a transmitter device 400 in accordance with the invention and suitable for use in a key fob. It comprises receiver (Rx) 470 coupled to a receive antenna 480 for detecting the magnetic field M emitted by the in-car device. An output of the receiver 470 is coupled to an input of a control means (μC) 410, and an output of the control means 410 is coupled to an input of a transmitter (Tx) 420. On detection of the magnetic field M , the control means 410 initiates transmission of the code signal s_j by the transmitter 420 which is coupled to a transmit antenna 430. The code sequences m_k for transmission in the code signals s_j are supplied to the transmitter 420 from a look-up table (LUT) 460. The selection of code sequence from the LUT 460 for transmission is made by a modulo N counter 450 which is coupled to address the LUT 460. The modulo N counter 450 is clocked by a clock (CLK) 440 and counts 0 to $N-1$ cyclically. The duration of each code signal s_j is dependant on the duration of the code sequences m_k , and on the number of code sequences transmitted in each code signal s_j , which may be varied by the control means 410.

Referring again to Figure 3, in the receiving device 200 reference code sequences, identical to the code sequences m_k stored in the LUT 460 of the transmitter device 200, are stored in a look-up table (LUT) 260 which is coupled to the detector 160, and reference code sequences are supplied to the cyclic register 167 thereby forming the reference code signal.

The constituent elements of the detector 160 are adaptive to detect code sequences m_k of different durations, and the processing means 210 is adaptive to determine the time of flight for code sequences m_k of different durations.

The selection of reference code sequence from the LUT 260 for correlation is made by a modulo N counter 250 which is coupled to address the LUT 260. The modulo N counter 250 is clocked by the clock (CLK) 240 and counts 0 to $N-1$ cyclically. The clock 240 is coupled to the processing means 210 and can be adjusted in response to the detection of the received code sequences m_k in order to synchronise the clock 240 with the corresponding clock 440 in the transmitting device 400. In this way, the choice

of which code sequence m_k is transmitted and received is dependent respectively on the current value of the counter 450 of the transmitter device 400 and the counter 250 of the receiver device 200, and the decoder 160 is maintained in synchronism to correlate for the code sequence transmitted by the transmitter device 400.

Provision may be made in case the counters 450, 250 in the transmitter device 400 and receiver device 200 become non-synchronised, for example due to an extended period without communication. One way of coping with this situation is for the receiving device 200 to correlate for a range of code sequences, instead of for a single code sequence m_k , the range of code sequences corresponding to the degree of non-synchronism likely. In this way, it can be ensured that the receiving device 200 will react to the code sequence mostly recently transmitted by the transmitter device 400, even though the receiving device 200 may have a margin of uncertainty over which code sequence is *a priori* being transmitted.

Other methods of selecting the code sequence m_k may be used. For example, the next code sequence m_k in a predetermined succession of code sequences may be selected for each successive transmission of the code signal s_j . If this method is used, the transmitter device 400 and receiver device 200 can become non-synchronised if the transmitter device 400 transmits a code signal s_j that the receiving device 200 fails to receive, perhaps because of inadequate signal strength. To cope with this situation, the receiving device 200 may correlate for a range of code sequences, instead of for a single code sequence m_k , the range of code sequences corresponding to the degree of non-synchronism likely.

It is not essential for the duration of the code sequence in every successive code signal s_j to vary from the duration of the code sequence in the previously transmitted code signal, provided that the duration changes sufficiently frequently to make unauthorised detection difficult. For example, the duration of the code sequence may be changed after transmission of a predetermined number of code signals or after the elapse of a predetermined time period, the change being controlled in the transmitter device 400 by either

the clock 440 or the control means 410, and in the receiving device by either the clock 240 or the processing means 210.

As a result of varying the duration of the code sequences, the duration of the code signal may vary proportionally. The number of repetitions of the code sequence within the code signal may be varied by the control means 410
5 to maintain an approximately constant duration of the code signal.

Similarly, the duration of the receiver time window may be varied proportionally with the varying duration of the code sequences, or alternatively the length of the buffer 165 and the cyclic register 167 may be adaptive to
10 detect an approximately constant duration of code signal.

Although an embodiment has been described using direct sequence spread spectrum sequences, alternatively the code sequences may comprise frequency hopping sequences.

The invention is not limited to keyless car entry systems and to systems
15 for tagging a person, animal or object, but may be used in other applications requiring wireless activation dependent on time of flight or propagation distance measurement.

In the present specification and claims the word "a" or "an" preceding an element does not exclude the presence of a plurality of such elements.
20 Further, the word "comprising" does not exclude the presence of other elements or steps than those listed.

CLAIMS

1. A wireless activation system comprising a first device (400) having means (460,420) for generating and transmitting a code signal, wherein
5 each successive transmission of the code signal comprises a successive code sequence from a succession of code sequences, and a second device (200) having means (210,240,250,260) for generating the succession of code sequences in synchronism with the first device, means (110) for receiving the code signal, means (160) for detecting the successive code sequence
10 transmitted by the first device, means (210) for generating an indication of the time of flight of the code signal, and means (210) for generating an activation signal in response to the combination of the detected successive code sequence corresponding to the successive code sequence generated most recently by the second device and the indication of the time of flight being
15 within a predetermined range of values, wherein the succession of code sequences comprises code sequences of different time durations.

2. A wireless activation system as claimed in claim 1, wherein the code sequences of different time durations comprise code sequences of
20 different symbol or chip durations.

3. A wireless activation system as claimed in claim 1, wherein the code sequences of different time durations comprise code sequences of different numbers of symbols or chips.
25

4. A wireless activation system as claimed in claim 1, 2 or 3, wherein the means (460,420) for generating and transmitting the code signal comprises means (440) for changing the time duration of the transmitted successive code sequence in response to the elapse of a predetermined time
30 period.

5 5. A wireless activation system as claimed in claim 1, 2 or 3, wherein the means for generating and transmitting the code signal comprises means (410) for changing the time duration of the transmitted successive code sequence in response to the transmission of a predetermined number of the code signals.

10 6. A wireless activation system as claimed in any one of claims 1 to 5, wherein the means (210) for generating the activation signal is responsive to the indication of the time of flight being below a predetermined limit.

15 7. A wireless activation system as claimed in claim 6, and wherein the second device (200) further comprises means (300) responsive to the activation signal for activating or deactivating a locking means.

20 8. A wireless activation system as claimed in claim 7, wherein the second device (200) further comprises the locking means (300).

25 9. A wireless activation system as claimed in claim 7, wherein the wireless activation system is a vehicle security system.

30 10. A wireless activation system as claimed in any one of claims 1 to 5, wherein the means (210) for generating the activation signal is responsive to the indication of the time of flight being above a predetermined limit.

35 11. A wireless activation system as claimed in claim 10, wherein the second device (200) further comprises means (300) responsive to the activation signal for generating an alert.

40 12. A wireless activation system as claimed in claim 11, wherein the wireless activation system is a system for tagging a person, animal or object.

13. A wireless activation system as claimed in any one of claims 1 to 12, wherein each code sequence comprises a spread spectrum sequence.

14. A wireless activation system as claimed in claim 13, wherein the
5 spread spectrum sequence is a frequency hopping sequence.

15. A method of wireless activation comprising at a first device (400) generating and transmitting a code signal, wherein each successive transmission of the code signal comprises a successive code sequence from a
10 succession of codes, and at a second device (200) generating the succession of code sequences in synchronism with the first device, receiving the code signal, detecting the successive code sequence transmitted by the first device (400), generating an indication of the time of flight of the code signal, and generating an activation signal in response to the combination of the detected
15 successive code sequence corresponding to the successive code sequence generated most recently by the second device (200) and the indication of the time of flight being within a predetermined range of values, wherein the succession of code sequences comprises code sequences of different time durations.

20

16. A method of wireless activation as claimed in claim 15, wherein the code sequences of different time durations comprise code sequences of different symbol or chip durations.

25

17. A method of wireless activation as claimed in claim 15, wherein the code sequences of different time durations comprise code sequences of different numbers of symbols or chips.

18. A method of wireless activation as claimed in claim 15, 16 or 17,
30 wherein the time duration of the transmitted code sequence is changed in response to the elapse of a predetermined time period.

19. A method of wireless activation as claimed in claim 15, 16 or 17, wherein the time duration of the transmitted code sequence is changed in response to the transmission of a predetermined number of the code signals.

5 20. A transmitter device (400) for use in wireless activation system, comprising means (460,420) for generating and transmitting a code signal wherein each successive transmission of the code signal comprises a successive code sequence from a succession of code sequences and wherein the succession of code sequences comprises code sequences of different time
10 durations.

21. A transmitter device (400) as claimed in claim 20, wherein the code sequences having different time durations comprise code sequences having different symbol or chip durations.

15

22. A transmitter device (400) as claimed in claim 20, wherein the code sequences having different time durations comprise code sequences having different numbers of symbols or chips.

20 23. A receiver device (200) for use in a wireless activation system, comprising means (210,240,250,260) for generating a succession of code sequences, means (110) for receiving a code signal, means (160) for detecting a code sequence conveyed by the code signal, means (210) for generating an indication of the time of flight of the code signal, and means (210) for
25 generating an activation signal in response to the combination of the detected code sequence corresponding to the code sequence generated most recently and the indication of the time of flight being within a predetermined range of values, wherein the succession of code sequences comprises code sequences having different time durations.

30

24. A receiver device (200) as claimed in claim 23, wherein the code sequences having different time durations comprise code sequences having different symbol or chip durations.

5 25. A receiver device (200) as claimed in claim 23, wherein the code sequences having different time durations comprise code sequences having different numbers of symbols or chips.

10 26. A receiver device (200) as claimed in claim 23, 24, or 25, further comprising means (240) to change the time duration of the generated code sequences in response to the elapse of a predetermined time period.

15 27. A receiver device (200) as claimed in claim 23, 24, or 25, further comprising means (210) to change the time duration of the generated code sequences in response to the generation of a predetermined number of the successive code sequences.

20 28. A receiver device (200) as claimed in any one of claims 23 to 27, wherein the means (210) for generating the activation signal is responsive to the indication of the time of flight being below a predetermined limit.

25 29. A receiver device (200) as claimed in any one of claims 23 to 27, wherein the means (210) for generating the activation signal is responsive to the indication of the time of flight being above a predetermined limit.

1/3

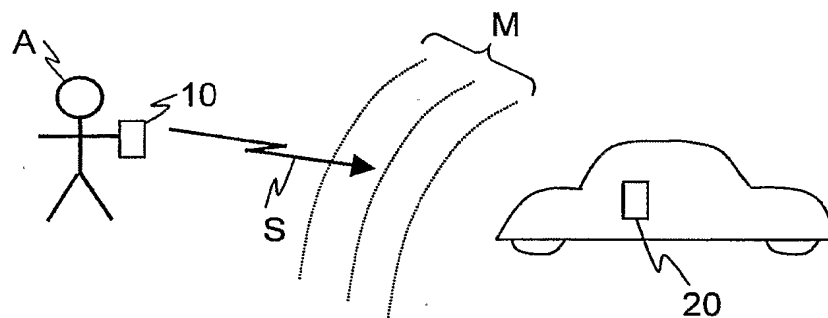


FIG.1

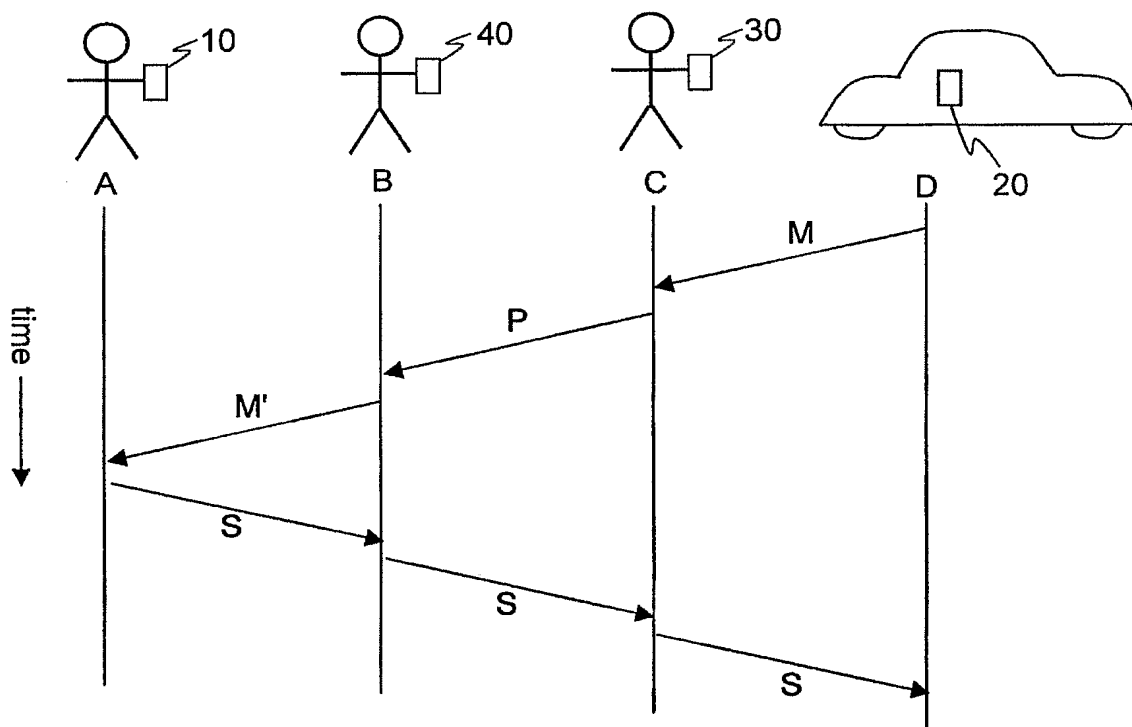


FIG.2

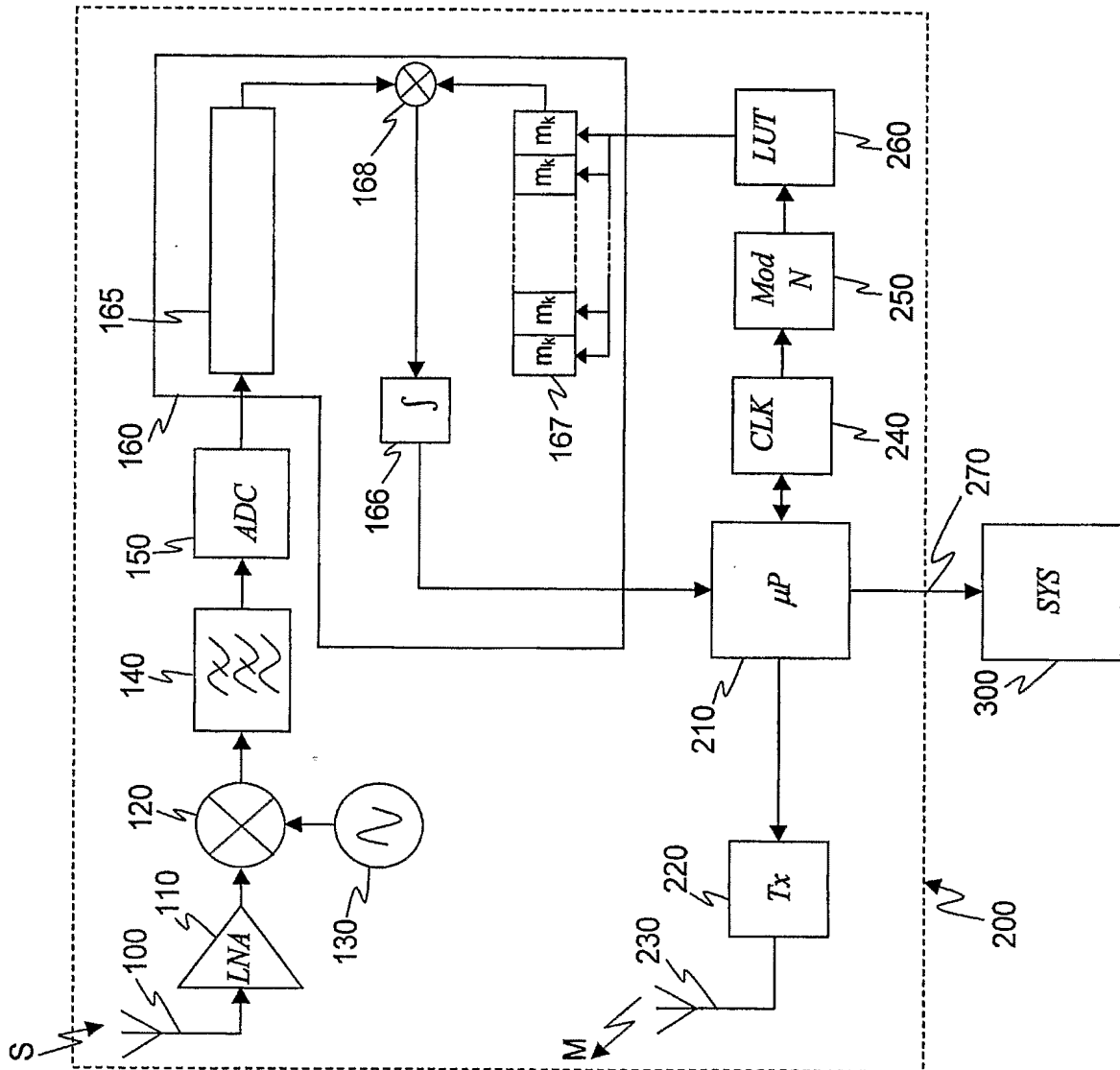


FIG.3

3/3

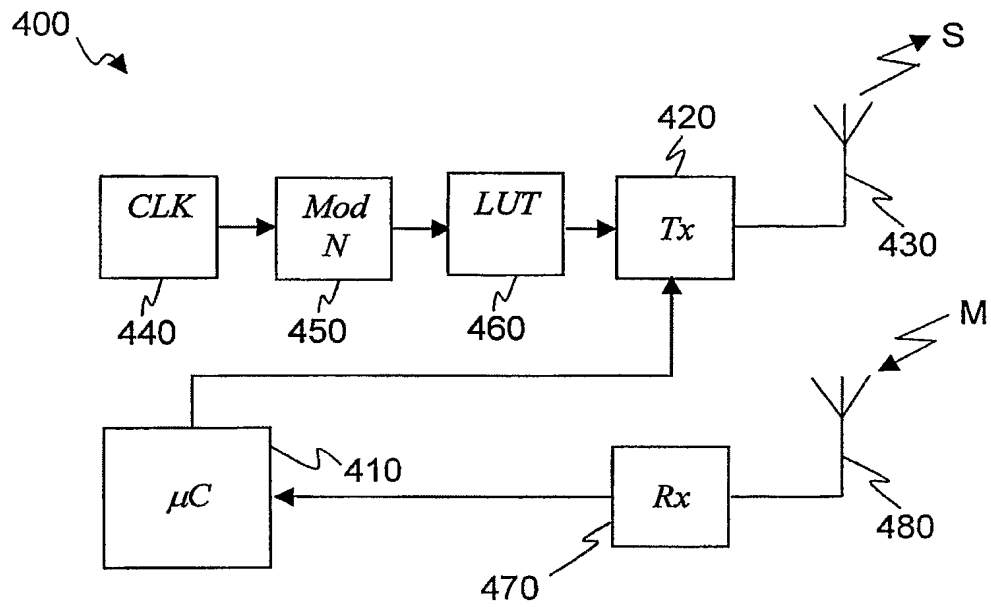


FIG.4

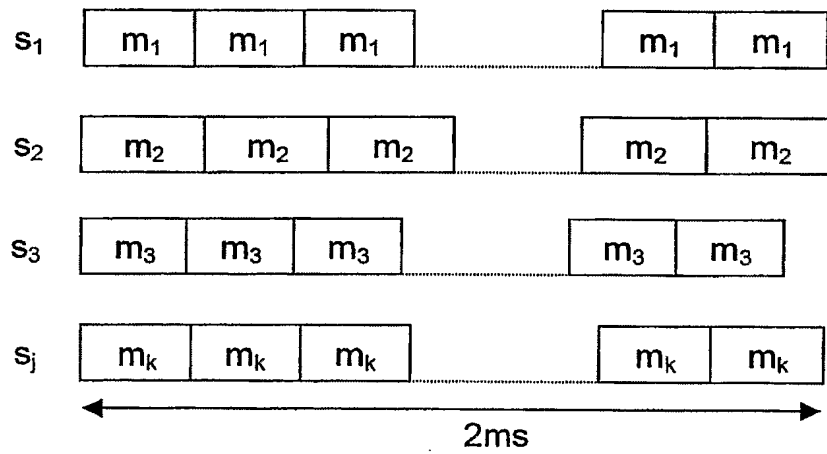


FIG.5